ASP Privacy & Security Policies

Access

How does your system ensure that only authorized users have access to only minimum necessary information?

CureMD utilizes advanced technologies to enforce strict adherence to privacy and security standards, including encryption, strong authentication, role-based privileges, granular security policies, and tamper-proof audit logs.
Access to CureMD is governed by a state of the art, multi-tier, role-based security model with functions driven by user rules specified in the system security module that regulates information such as access by function, information, role and patient chart as determined by practice administrators.

Authorization

How does your system authorize users to access information?

CureMD provides flexible and powerful role-based authorization mechanisms. Roles are defined for various levels of user access and assigned to users as required. User authorization is dynamically adjusted to cater for temporary or permanent operational variations.

Authorizations are regulated based on time and day login restrictions as well as IP address and login restrictions.

Authentication

How does your system ensure that the person accessing the system is who they say they are?

In addition to Award winning Key Stroke based Authentication as well as Finger Print authentication options, CureMD supports elemental authentication technologies needed to enforce a strong authentication policy. Users of CureMD EHR are prompted for a username and password. These credentials are sent (in encrypted form) using an HTTPS connection to the CureMD Gateway, which verifies the identity of the user by connecting to a Key Distribution Center (KDC). The KDC can be configured to enforce strict password policies, such as length and pattern of password and frequency of password change.

Audit

What audit procedures are in place that will promote transparency and compliance with access, use, and disclosure requirements?

CureMD provides flexible real time logging capabilities for all requests using a secure tamper-proof audit log. This data can be used to monitor usage of the system, to investigate any suspected misuse, and to conduct periodic audits.

CureMD audit trail provides full audit logging capabilities and display complete transaction history with user, date time, and IP recording. Modifications are highlighted for easy tracking.

Secondary Uses of Data

How does your system ensure that the use and disclosure of information is limited to appropriate and approved users?

By Meeting HIPAA compliance standards CureMD ensures all access to data, functions, screens, and records is password-protected and set by the security administrator through the flexible and powerful role-based authorization mechanisms. There is no secondary use of the data without the express permission of the client either.

CureMD does provides practices ability to re-use data for the purpose of benchmarking themselves against other physicians and their quality of care in order to get reimbursed (PQRI Reporting).

Data Ownership

Where is the data stored and who owns the data?

For SaaS/ASP Solutions: Data is stored at SAS70 certified data centers or secure hosting locations.
For Client Hosted Solutions: Data is stored at client location. Backup/Mirror services are available as optional.
For both solutions, the client owns their data.

Sensitive Protected Health Information

Sensitive health information refers to select protected health information (PHI). Federal and state laws impose heightened privacy and security requirements upon the disclosure of certain types of PHI that may be considered particularly private or sensitive to a patient such as genetic information, psychotherapy notes, substance abuse treatment records, etc.

Vendor did not provide additional information.

Yes	No	
☑	☐	*Does your system have the ability to identify PHI that is sensitive?*

If yes, explain: Yes

Yes	No	
☑	☐	*Does your system have the ability to prohibit sensitive PHI from being shared electronically?*

If yes, explain: Any user can be restricted from accessing any patient chart

Yes	No	
☑	☐	*Does your system have the ability to break the glass (Break the glass refers to the ability to obtain health information in emergency situations where consumer consent has not been granted)?*

If yes, explain: Break the glass option can be granted to User restricted from accessing a patient's chart.
Upon availing facility (breaking glass) all activities are logged into the system.

Consumer Accounting of Disclosures

How does your system generate reports for consumer of access to their records?

CureMD EMR generates reports with healthcare quality measures that can be used to track progress in achieving provider and practice quality measure.

CureMD's EMR authorization is a process in which the system protects resources by only allowing them to be used by authorized resource consumers. Patients authorization is required to give authorization to some figures to access their data. CureMD EMR Integrity prevents data to be created or amended without the right authorization.

Secondary Data Use

Does your EHR system have provisions which allow the EHR vendor to extract a Limited Data Set of patient information to use for research purposes by the EHR vendor or a third party, if the practice agrees to participate in a study?

Yes (optional service and is subject to HIPAA compliance)